Privacy and Security Tiger Team
Draft Transcript
May 23, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good afternoon, everybody, and welcome to the Privacy and Security Tiger Team. This is a Federal Advisory Call, so there will be opportunity at the end of the call for the public to make comment, and please, just a reminder for workgroup members to identify themselves when speaking.

Let me do a quick roll call. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Egerman?

Paul Egerman – Software Entrepreneur
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Dan Rode is speaking.

Dan Rode – AHIMA – VP Policy & Government Relations
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Gayle Harrell is boarding a plane so she probably won't be able to join. Carol Diamond? Carl Dvorak?

Carl Dvorak – Epic Systems – EVP
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
David McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Neil Calman? David Lansky? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Micky Tripathi? Christine Bechtel? John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Wes Rishel?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Leslie Francis?

Leslie Francis – NCVHS – Co-Chair
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Vern Ranker? Lisa Tutterow?

Lisa Tutterow – Office of the National Coordinator – popHealth Principal
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Deborah Lasky?

Deborah Lasky – ONC
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Did I leave anyone off?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Carol Diamond is here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. I'll turn it over to Deven and Paul.

Deven McGraw – Center for Democracy & Technology – Director
Paul, take it away.

Paul Egerman – Software Entrepreneur
Yes. Thank you very much Deven and Judy. Good afternoon or good morning for those on the west coast, so this is a conference call of the Privacy and Security Tiger Team. We are a group of individuals from the Policy Committee and Standards Committee and other people and we provide policy advice on a series of policy and security issues. If you listened to the roll call, you may have heard, we added one person for our discussions on … that we're going to do in a few minutes. That's Dan Rode, who is a Vice President of AHIMA, a great organization, so we're happy to have you join our team Dan.

Dan Rode – AHIMA – VP Policy & Government Relations
Thank you.

Paul Egerman – Software Entrepreneur
Briefly review our agenda, we have a number of very interesting topics that we are going to be going through today. First, we did have a request through the ONC blog for feedback on topics, and we want to review those issues. We have put forward a tentative agenda for what we're going to discuss over this summer and some issues that we put like, we called it on deck, for issues for later in the fall. The agenda you see on your screen then says strawman recommendations on corrections and amendments. We're actually going to do an agenda item that's not listed on this screen that sort of happened at the last minute before that, which is we're going to review the certificate authority recommendations from the task force to just refresh everybody's memory. There was a sort of a dangling issue, a piece of unfinished

business on certificate authorities from our previous recommendations that the Standards Committee asked us to address. We put together a task force to address that issue, and that was under the leadership of Dixie Baker and David McCallie, and being overachievers, they actually got their work done early, and so they will be presenting that material. So, we'll be hearing that, and then we will dive into the issue of corrections.

Before I go on and start to enter the next item, the blog comments, did you have anything that you wanted to add, Deven?

Deven McGraw – Center for Democracy & Technology – Director
No. You can go right on.

Paul Egerman – Software Entrepreneur
Okay. So the blog comments, I don't know if there's any way to bring them up on this screen.

W
Yes. Is that the amendments corrections PDF?

Deven McGraw – Center for Democracy & Technology – Director
No. It's the other one.

W
Okay. Yes. I can bring that up right now.

Paul Egerman – Software Entrepreneur
Yes. Terrific, so--

W
First we need magnifying glasses, right?

Paul Egerman – Software Entrepreneur
If people are able to make that full screen, that may be helpful to you. Or either that or I just encourage you to go real close to your screen. But as Judy Sparrow said when we opened this call, the public comments are critically important part of our work, and so we had this request for guidance on the ONC blog and this is what you see here it says public comments on suggested priorities is the summary of the feedback we got. We got a lot of feedback, and this is all extremely helpful. So you see that first under the section of public comments. Then, what you see underneath that document is, I'm scrolling forward and hope that scrolls forward for everybody.

W
It is. It is, Paul.

Paul Egerman – Software Entrepreneur
Terrific. So you see where it says Tiger Team Priorities. This is original priorities and then we see put in red is how we alter that as a result of the public comments. So, what we basically did was the first issue that we had was completing the policy framework for push transactions. It says corrections and other data integrity issues beyond patient matching. Then, we added based on the public comment, transparency of the original source and dates of data in the record. Then, we had query and response models of HIE and we added additional business associate issues specific to HIOs. Then we have issues associated with hosted EHRs, patient portal issues, HIPAA Security Rule gap analysis, internal unauthorized access, which is an issue raised by Neil Calman and a few other people. Then we also added provider and consumer education on definition and use of de-identified data. So that is how we are responding to the comments we received on the blog. Then, before I talk about how we're going to schedule that, let me pause and see if people have any reaction to that material.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Hey Paul, the very last one, provider and consumer education on the definition and use of de-identified data, something has come up and I talked to Deven about a little bit was related to limited data sets. I suspect that limited data sets and data use agreements might be something that also come up in the context of ... and the like, and I'm just wondering whether we should be also talking about limited data sets as well as de-identified data.

Deven McGraw – Center for Democracy & Technology – Director
I wonder if we should have had secondary, I'm trying to remember where we scheduled it, secondary data usage as a big topic to take on in the future. We may not have parking lotted it but to me that's a limited data set being a vehicle for secondary data use is better discussed in that context because they're not, even though they're both limited data set and de-identified data are data stripped of identifiers, one is PHI and the other is not. So I'm not sure they belong together in the same bucket, but I do think that the limited data set discussion from a secondary data use perspective is an important one.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
My only concern is that we at least talk about de-identified data here. The assumption is that there aren't issues with limited data sets and my fear is, is that there are also issues with limited data sets or concerns yet limited data sets actually contain more information yet aren't really going to be talked about within the framework of the discussion about de-identified data.

Deven McGraw – Center for Democracy & Technology – Director
Well right. Because one's regulated and one's not.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Right, and so we end up not talking about the one that's probably more, what's the word, more sensitive or could have more issues if we just said we talked about de-identified data.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Why don't we, I think as you'll see when Paul gets to the schedule, we've got de-identified data on deck for the fall so we can just make a note about whether limited data sets should be added, would be my suggestion.

Paul Egerman – Software Entrepreneur
Also, John, to be clear, this topic that's in red here, is really about education. It's provider and consumer education on definition of use. It's actually not on privacy and security policies, it's simply a discussion about do people understand what's going on.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Right.

Paul Egerman – Software Entrepreneur
It's just two different issues. Do people understand what's going on? And the second issue is what should be going on.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
And to telegraph my concern is that I am seeing more and more business associate agreements where business associates are trying to reserve the right to create their own limited data sets on their own behalf and for their own purposes. I don't think it ever contemplated that but it's a huge concern of mine.

Paul Egerman – Software Entrepreneur
Yes, it's a good issue. So let's, exactly as Deven suggested, let's revisit that when I get to the schedule.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Thank you.

Paul Egerman – Software Entrepreneur

So good issue, John. Other issues? Any other comments about where we are with the tiger team priorities?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Paul, what is the business associate issue, are the business associate issues?

Paul Egerman – Software Entrepreneur
Specific to HIOs, good question.

Deven McGraw – Center for Democracy & Technology – Director
What are you referring to Dixie?

Paul Egerman – Software Entrepreneur
It's underneath query and response models of HIE, this sub bullet in red, additional business associate issues specific to HIOs.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I think people have asked us since that was an addition. My recollection from the blog is that people have asked us to go back and look at an issue that we keyed up. In our summer letter where we acknowledged, we put out an entire set of fair information practice requirements on all entities involved in exchange including but not necessarily limited to HIOs and then specifically acknowledged that business associate agreements were one vehicle for providing some limitation on how a BA could use data. But it probably wasn't sufficient because of the power dynamic associated with some business associates being bigger players in the market place than the covered entities that they serve. So since HIOs are required to be business associates, I think it was just a placeholder for the issue of regulating that, whether our business associate agreement is a sufficient regulatory vehicle to take care of some of those issues. Some of which, again, we've already keyed up.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So what you're really talking about is business associates, is issues relating to HIOs as business associates rather than business associates using HIOs.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Paul Egerman – Software Entrepreneur
That's correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay got it. Thank you.

Carl Dvorak – Epic Systems – EVP
Paul and Deven one of the comments that came up at the meeting week before last was about the acquisition of the HIE vendors by the insurance companies and people had a general sense that was something to look into, but I'm not sure what exactly one would look into about that. But I do remember that that came up, so I thought I would just mention here because I don't see it on this list and maybe it's not appropriate for this, I don't know.

Paul Egerman – Software Entrepreneur
It's an interesting issue, Carl, the question is what role would we play on that issue though.

Carl Dvorak – Epic Systems – EVP
Yes, I don't know. I just thought I'd mention it since it came up last week.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It did.

Carl Dvorak – Epic Systems – EVP
... more to say about it than that.

Judy Faulkner – Epic Systems – Founder
I have an experience that was last week when the CEO of a bank told me that their tellers are reviewing the payments made to different organizations and suggesting maybe that instead of using one bank, they might want to use their bank or these service instead of those services. Which I and another person in healthcare both were shocked that it was a violation of personal information, and the banker didn't think so at all. As we get into these various business associates agreements with different groups there, I think that the really interesting thing was that he didn't see it as a violation and what will these folks think is and isn't the right thing to do with that data that goes through them now. Because one thing to say is that they're buying them because they just want to get into another business. Another thing to say is they're buying them because they want the data.

Paul Egerman – Software Entrepreneur
Those are helpful comments. I'm wondering if I've listened to what you just said Judy and thinking about what Carl said and also what Dixie said, I'm wondering if these are issues that we could address as part of that whole discussion about business associate issues and HIOs and query response issues.

Judy Faulkner – Epic Systems – Founder
Well I know that the insurers have come to us many times for will we share the data with them and our answer has been always it's not our data to share and number one. And number two, that for the most part, we see a lot of physician and provider organizations very concerned about sharing that data. So it's a very interesting new thing we're seeing with the purchase of the HIE information organizations.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. I guess the question that comes to mind here is whether data is shared under HIPAA is shared, is limited to the purposes for data sharing that don't require patient consent. If so, then the issue is are people being naïve in believing that Aetna could mine patient data from an HIE stream or if it's not so clear then it needs to be done. I suppose the reason the chairs are questioning the relevance to this committee is because it's a HIPAA issue. I would just say that if our description of our information practices are not clear on this point, they should be. If they aren't consistent with HIPAA we should be making a note of that.

Paul Egerman – Software Entrepreneur
But what, I'm trying to understand. I sort of understand the issue and I appreciate what you're saying Wes, but my question is, is the way to handle this as part of our discussion about business associate agreements with HIOs or is that—?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well I think that what we've heard what's been refined through the contributions is that the driver behind that comment is the notion that limited data sets somehow get a different ride than protected data in terms of the ability of the business associate to use that for something other than the purpose of the— In other words, if I'm a hospital and I use a business associate to generate safety data or something. I understand that I give that information to the business associate for that purpose not for it to go ahead and use that data for whatever else it wants. At least, that's my understanding of how HIPAA works.

Deven McGraw – Center for Democracy & Technology – Director
Yes. That's my understanding too, Wes. I think we want to be careful in this discussion of future topics not to start into the substance of discussion. But I think you're right that when we get into this category, we're going to have to really have an understanding from our staff at OCR who help us, what the rules are under HIPAA regarding business associate use of data and what they are not so that we can very carefully construct our recommendations and acknowledgement of that. Because I think there's a lot of potential misinformation out there.

M
And Deven, there was one, there's only one place in the ARRA regulations that I vaguely remember that talked about this but it was the notion that one would be able to pay cash for medical services and to not have it reported to its insurance carrier. I think that made it through to the final.

Paul Egerman – Software Entrepreneur
Yes, it did.

M
And I think the only concept I see is that the insurance carrier can impact also the HIE. We might want to have some thought on how to handle the HIE where that is the case ... and the HIE are one in the same.

Leslie Francis – NCVHS – Co-Chair
Deven, to the extent that de-identified data is also being used and I think it's there as much as or even more than limited data sets, make sure it, that the discussion covers that issue too. The identified data sets by business associates.

Paul Egerman – Software Entrepreneur
So are we putting this entire discussion as sort of like part of the discussion of de-identified data and limited data sets.

Deven McGraw – Center for Democracy & Technology – Director
No I think it's crossed over into also HIOs and business associate agreements and who owns HIOs. We're going to have to do some offline parsing about what fits into what discussion, would be my suggestion. There is obviously some interplay among all of these issues.

Paul Egerman – Software Entrepreneur
Okay. Well these are helpful comments. And appreciate people bringing them up because we do want to respond to those issues. They're critically important. So I'm going to move on next to then how we're going to schedule these items.

Let me jump on the next page if that comes up. Yes. So what we tried to do was to put together a schedule for all of our meetings through the summer, and so that's what you're seeing on your screen. So today's meeting, it says continue corrections. June 3rd says report on Certificate Authority Task Force. Actually, we're going to do that today. So then, we'll probably continue corrections other issues related to data integrity and quality, and then you have the Policy Committee meeting and as you can see, we basically did our best to sort of slot every meeting through August. We sort of stopped at August because, we didn't want to, it's sometimes very difficult to figure out how to schedule. Some topics take a lot longer than you expect. Some topics go a bit faster. So then what we did was for what we call the fall topics, we just listed these items that you see down here are patient portal issues beyond security, HIPAA Security Rule gap analysis, internal unauthorized access, which is again an issue Neil raised, and then we have provider and consumer education on definition use of de-identified data. And if I'm hearing this discussion right, we probably want to add on to fall topics, some discussion about these issues of limited data sets and the business associate agreements.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
So Paul, with regards to the second bullet, I'm actually thinking about this. Is there any interest in working a HITRUST because you talk about HIPAA and other industry standards. I know HITRUST is intended to try to help bridge the gap between the various rigs that providers have to comply with. Does that make sense to try to include HITRUST under instruction or is that way beyond the scope?

Deven McGraw – Center for Democracy & Technology – Director
Put HITRUST under discussion of what specifically, John?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

HITRUST is supposed to be an amalgam of a bunch of different security regs that relate to health care and I'm wondering whether that's a—

Deven McGraw – Center for Democracy & Technology – Director
I only think that approaches from industry groups are helpful when we are taking up certain topics to learn from their approaches. I remember we had some folks from ... for example on another set of issues, forgive me for not remembering which ones those were. So if you want to circulate them, I think rather than having dedicating a meeting to ... we might sort of look to them and any others that members of the public share with us as potential ideas for recommendations on how to go forward.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I'm just thinking HITRUST might provide a good comprehensive view of health care information.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think they might but I think we have to remember that they are a trade association. They're not a—

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I understand.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
They're not anything else right now.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
That's why I bring it up. I mean, we can say no to it. I just, you know, we might at least use them to understand maybe what other regs are applicable that we might ....

Deven McGraw – Center for Democracy & Technology – Director
Anybody is always welcome to and most of them do forward to us suggestions of approaches that we can take, so—

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Okay, fair enough.

Paul Egerman – Software Entrepreneur
So this is the tentative schedule. As you see, the month of July is when we're talking about some of these HIE models. This might be one place that we might conclude some of the discussion we just had on the topics of relationship between the HIE software and insurance companies and business associate agreements might occur in the month of July. But we also might want to schedule some of them at the fall as it relates to limited data sets and secondary uses of data. I'm not sure about that one issue. Do we have other comments about this agenda? Does it look reasonable to people?

Deven McGraw – Center for Democracy & Technology – Director
As always, I think we're ambitious, but I think we've managed to do really well from our, in the past. So and I like setting the bar high.

Paul Egerman – Software Entrepreneur
Okay. Any other comments? So that's great. So what we have is terrific. We have a whole series of very interesting topics, and we have an ambitious schedule so we've got our work cut out for ourselves. That's good I guess. That's why they still call us the tiger team. So terrific. So that completes the discussion about the blog and the schedule going forward. The next item that wasn't really on the agenda but that we wanted to do was the whole discussion of the recommendations from the task force on the certificate authority so if we could ask to queue up the, there's this really short slide deck that Dixie did. Dixie can take us through that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay. Paul is right. Just to remind you, we were sent, this tiger team was sent an assignment from the ONC or from the Standards Committee by way of the ONC to recommend policy around how to get some minimal level of assurance in the certificates, certificate authorities. To refresh your mind, certificate authorities are the organizations that issue digital certificates that are then used for authentication purposes as well as digital signatures. So we were given, this task force was given the charge of recommending the minimal assurance required for certificate authorities that issue digital certificates for use in the exchange of health information within the nationwide health information network.

So, next slide. A key consideration— You went too far.

<u>Paul Egerman – Software Entrepreneur</u>
This is the second. That was the first one. This is your second one.

<u>Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences</u>
Okay she went too far the first time. Okay. The options that we identified were first that the CAs could operate under more of the governance of the ONC. The second option, which is one that's a Direct project is to require that the CAs conform to best practices that have been established by WebTrust and the European Telecommunications Standards Institute, which also do accreditation CAs. The third option is that the CAs would be cross-certified with the Federal Bridge Certificate Authority either directly with the Federal Bridge CA or cross-certified by a CA that was cross-certified by the Federal Bridge.

So, next slide please, three. So the considerations that we discussed, first consideration is that is the recognition that virtually every health care organization will at some point need to exchange health information with a federal agency, whether it be the VA, the military health system, CMS or the Indian Health Services. And under the federal law and the federal CIO counsel, federal agencies, a federal agency really is required to accept certificates that are cross-certified with the Federal Bridge CA, which I've abbreviated FBCA right there. With Deborah Lasky's help, she talked with several agencies and asked them about the three options that I just went over and asked them what their current policy was, what they thought was required for an exchange between a private entity and a federal entity. None of the agencies she asked said that they would accept a certificate that was issued by a CA that was not cross-certified with the Federal Bridge CA. As an example, the VA is participating in the direct project pilot and even in those pilots, they require that the certificates be cross-certified with the Federal Bridge.

The final consideration is that we learned, Deborah learned, that the Federal PKI policy has been established, that they have established a Citizen and Commerce Class Common Certificate Authority, what they call the C4CA that is cross-certified with the Federal Bridge CA for exactly this purpose. And this is relatively new policy that just was released in August of last year that says that if they're a private entities and they're exchanging information with a federal agency that they will be able to get certificates from the C4CA Certificate Authority that is cross-certified with the Federal Bridge and manage them with the governance of federal policy.

So, slide four. So our recommendation is that all certificates used in NwHIN exchanges must meet Federal Bridge standards and must be issued by a CA that is a member of the Federal TKI Framework. We stated it this way because we recognize that there are several ways to address this. One is to get a certificate from a CA that is directly cross-certified with Federal Bridge CA, but the CA also might be cross-certified with a health bridge that would be cross-certified with the Federal Bridge CAs. A number of these other bridges that are cross-certified with the federal bridge already exist. In fact, one of them is the SafeBiopharma Bridge CA. So the third option is that the CA could get cross-certified with an existing Bridge that's cross-certified with the Federal Bridge. Then the final option, and these are options for certificate issues distributors. The fourth option is to not become a CA at all but to obtain blocks of certificates from a cross-certified CA and then to redistribute them under the governance of that CA. So that is our recommendation.

<u>Paul Egerman – Software Entrepreneur</u>
Great job Dixie. Questions? Do people have questions, comments?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So the fourth option there sounds a lot like saying here we'll give you the keys to the jail and you can give them out under whatever your rules are. Who's governance, which CA is the governance here? Can you explain that more? It sounds kind of kinky to me.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Governance is established by the CA that distributes the certificates to begin with, so the CA here is cross-certified with the Federal Bridge and it inherits the rules from the Federal Bridge CA. So the Federal Bridge CA rules still apply. It's just that instead of having to go through the process of becoming a CA themselves, the issuer say a HIST for example, in the Direct Exchange would instead just obtain the certificates from a cross-certified CA. Then, in accordance with the rules established by that CA and in accordance with the rules established by the Federal Bridge, they would distribute those certificates to their members.

Paul Egerman – Software Entrepreneur
Or perhaps, Dixie, would another example be that a vendor like say Cerner or Epic—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Or even Health and Human Services. This is exactly the model that Health and Human Services—HHS does not have its own CA. They purchase blocks of certificates from a certificate authority that is cross-certified with the Federal Bridge and they then distribute them within Health and Human Services.

Paul Egerman – Software Entrepreneur
Yes. But the reseller concept would work. Say for example, a new customer, for example, Cerner or Epic, could ask their vendor, vendor installs the software to obtain the certificate for them, whereby they would get a certificate for ... or somebody who's cross-certified with the Federal Bridge. Is that correct Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But the rule's still apply. You still can't just distribute them without the rules. The rules come with the certificate.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So I guess, I think it's very helpful to have the two examples of a vendor and DHHS here to understand it. But what is required by the issuing CA in terms of assurance that someone who buys a block of certificates is in fact following its governance? Is it just, is it like the original concept of a business associate agreement where you tell me they're not and I might have to do something about it or is it, is there some proactive requirement? I just, I can see the possibility for some purchasers of certificates to be more nefarious than they seem on the surface. That's all I'm saying.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't know the answer to that. I know that if I were a CA and I were issuing blocks of certificates, it's a, their own integrity is on the line. So, I would want to be proactive, but we can find out what they generally do. We can find out what HHS does or any of these organizations.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
What I'm interested in is, what are the obligations and consequences that fall on the CA if one of their purchasers of blocks of certificates misbehaves?

Deborah Lasky – ONC
Dixie, would you like me to address that question?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Thank you.

Deborah Lasky – ONC

Sure. Wes, in reviewing the requirements to become a reseller, the agreement that the reseller must execute is fairly standard, and it places the burden on the CA to maintain the integrity of the process. So, they are proactively required by the root certificate authorities who are the ultimate links back to the integrity of the system. They're required to do audits. There are procedures for revocation of certificates that were obtained illegitimately and for revoking the rights of a reseller. But there is an investigative process that any prospective reseller has to go through before they are allowed to redistribute authentication credentials. It's a much higher standard than is required for example to just get an SSL certificate for email or for a website. But to be a reseller is a highly ... process. That said, there has been recently, well there has been at least one case where a registry authority who is responsible for authenticating a reseller has, whether inadvertently or on purpose, certified the identify of a reseller who was not who they said they were. So there were some questions around that, but if you fall back on the requirements of the Federal Bridge which are set at a very high standard of integrity, then the chances of that are greatly reduced.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you Deborah.

Deborah Lasky – ONC
Your welcome.

Deven McGraw – Center for Democracy & Technology – Director
I think that's extremely helpful to know. I'm really glad that Wes asked that question because I think we have to remember that the context for consideration of this issue in the first place was that we were worried about certificates for health exchange not being issued in a way that we could count on since patient data was at stake. So again, as Paul pointed out, we had initially said look ONC ... you a credit certificate authorities. This process seems to me to be a proxy for what we had identified as a process for vetting CAs, and in fact, even though it's not perfect as Deborah pointed out, may actually be better than asking ONC, which doesn't actually have any experience with managing certificate authorities, to accredit them.

Deborah Lasky – ONC
We're always up for a challenge.

Deven McGraw – Center for Democracy & Technology – Director
I think you've got a lot of them already.

Paul Egerman – Software Entrepreneur
So, Wes raised this issue about resellers. Deborah and Deven responded on the reseller issue. Are we comfortable with that response?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I'll speak a little bit for the Direct Pilot users and say that I think this is a promising avenue to explore, that the reseller approach sounds and looks like an approach that would be consistent with high standards of cert authority balanced against the cost of deployment of these certificates. But the proof will be in the pudding as we go through the next six to eight months of rolling out Direct, but I think this is a good starting point.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So, David, I understand that there may be some concerns about how this drives up the cost of products in essence, is that right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. There's Direct has from the beginning had a strong focus on the small practices that may not even be EHR enabled yet. And maybe it's for rural and underserved communities that might not have access to more robust HIE in their community. So that's only been one of the targets for Direct, and I think there's a strong desire not to exclude them by some inadvertent decision that pushes the complexity or

cost too high. So what's not known yet, to me anyway, is at, at scale what do these reseller certificates cost? And we'll have to see, but given the rules that Dixie discovered or that Deborah helped us discover around the approaches that the federal partners have to take and given that this is NwHIN is a federal branded exercise, it's going to have the federal M for mature on it, I think this is where we have to start.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Whatever David said, I agree with.

Paul Egerman – Software Entrepreneur
Okay so and to make sure we're all on the same page, Dixie and David are presenting this to us. If we approve it, then the next step is we're going to take it to, Deven and I will take it to the Policy Committee on June 8th and ask for the Policy Committee to approve it. So that's the path we're on. So, if people are uncomfortable and have any reason they don't like this, we need to, this is your chance to speak up. Are there any other concerns or questions about this?

Deven McGraw – Center for Democracy & Technology – Director
I do think that we will be well served in presenting this to the Policy Committee if we add a couple of slides with some of the information that Deborah Lasky provided to us about the soundness of the process for CAs and for brokers.

Paul Egerman – Software Entrepreneur
Okay.

Deborah Lasky – ONC
If it would be helpful, we also in doing this research collected some information on the cost to the end user.

Paul Egerman – Software Entrepreneur
It might be helpful. That's not really what's in our, directly within our scope.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'd be interested to hear what she has to say about it.

Paul Egerman – Software Entrepreneur
Okay.

Deborah Lasky – ONC
So in speaking with SafeBiopharma, the price that they stated to us for an end user certificate if purchased in bulk is $24 for a one-year certificate, and it would be slight less with using their online identity proofing. The cost for a notary driven process where the end user would have to actually appear before a notary, of course, would include the cost of the notary and the cost of the time involved. But for basic certificate, it's $24. Some other providers are "a little bit higher." The highest cost we saw was $109 for a one-year certificate, and the average seemed to be approximately $45.

Paul Egerman – Software Entrepreneur
That's helpful. Deborah, but the most important thing is there's multiple sources to get these certificates, right?

Deborah Lasky – ONC
There are. There are at least a half dozen.

Paul Egerman – Software Entrepreneur
So hopefully competition and supply and demand will cause this to have reasonable prices, although those prices seem easy for me to say because ... the owners to me.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Deborah, that's very helpful. Did they make any distinctions or did you ask any distinctions about the difference between individual versus organizational certificates?

Deborah Lasky – ONC
They generally don't distinguish. Their classes of certificates are distinguished between server-based certificates and identity-based certificates. So they don't really distinguish between organization and individual in their pricing.

Paul Egerman – Software Entrepreneur
Let's make sure that we stay focused on what our topic is for right now, which is as Dixie said, we were tasked with establishing and determining the qualifications of the certificate authorities to whom may issue these certificates. So, that's what we're addressing through this topic. So what you just told us Deborah and the response to the questions was useful information.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Paul, if you're implying it's not pertinent, then I disagree. But since we've already added the information, I guess that's—

Paul Egerman – Software Entrepreneur
You're just trying to find out make sure this is a solution.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If we had ended up recommending a gold-plated solution that cost every doctor $100 a month, then I don't think we have been doing anybody any good. So I think we have more conscience in the choice of the approach now.

Deven McGraw – Center for Democracy & Technology – Director
I agree.

M
Agreed.

Paul Egerman – Software Entrepreneur
Okay. So, are there any other comments you want to make on this topic? Am I correct in assuming then that this, a recommendation the task force is accepted by this tiger team?

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes.

M
Yes.

M
Yes, David.

W
Yes.

Paul Egerman – Software Entrepreneur
Terrific, so thank you Dixie. Thank you David McCallie. Great work, and Carl Dvorak, and we appreciate everybody's and of course Deborah Lasky.

M

Don’t forget Deborah did a huge amount of leg work.

Paul Egerman – Software Entrepreneur
Deborah actually did a massive amount of work, so thank you very much Deborah. Very interesting topic. So our next topic is corrections and amendments. I suppose we could look at what we just did as a correction and amendment or an elaboration on a previous certificate authority or recommendation but next topic is correction and amendments. Did you want to take us through that, Deven?

Deven McGraw – Center for Democracy & Technology – Director
Yes. Thank you very much Paul. I appreciate it, and thanks again to all on the successful recommendations on the certificate authority issue and for the hard work that everyone did to get us to this point in a really prompt way. It’s great to be able to report that to the Policy Committee. So we don’t have slides for this next set of discussions around corrections and amendments. What we distributed to the tiger team and which members of the public you can see on the left, there’s an amendments and corrections PDF is what is the—Oh, look at that. She put it right up there. That’s terrific, Katelyn, thank you. A document that inevitably we will, sets up some strawman recommendations that inevitably having it in the document form, quite frankly, is easier for us to turn into a transmittal letter of recommendations once we’re done. Then, starting with some bullet point slides and having to craft the letter after the fact, we’ve had, I think some success in getting recommendations through the Policy Committee that sometimes are quite complicated. When we present them in a form where they can be discussed more completely in text and the Policy Committee has an opportunity to read them in advance. So we’re continuing along that vein. We have addressed documents at the team for MITRE who provides us with so much assistance on all of these issues helped to prepare for us.

In essence, we sort of could divide into three big buckets. The substance of policy and technical issues that are really dealt with in this paper. With respect to policies on amendments and corrections, there are really two categories. One is, what are the sets of obligation? One bucket is around individual requests for amendment. So what does a provider entity need to do when an individual makes a request for a correction or an amendment? As we talked about on our last tiger team call, HIPAA really does provide quite a bit of substance in process that covered entities must follow in responding to requests from an individual for an amendment. It’s in a fair degree of detail, and we actually have, MITRE has replicated that for us and for those of you who either printed this paper out or can see distinctions in five colors on your screen, the information that comes from HIPAA is really in grey text and anything that we added additionally is in darker bold. When I say we added, meaning, again, this is a strawman discussion document that we are preparing for tiger team consideration and discussion. So the issue of patient request for amendment really takes up a considerable amount of this paper because in fact, there is so much detail in the HIPAA regulations.

But the other second bucket of issues, which we identified on our last tiger team call and for which we don’t have guidance from HIPAA is what happens to an error that doesn’t come. What happens with respect to a correction or an amendment that doesn’t come necessarily from an individual request from a patient but is instead discovered by a provider in the course of business. And what should be the set of substantive policy recommendations that we might make in order to ensure that errors in the record that are discovered get corrected. So beginning on about page four of your document if you print it, but the category begins principles for other changes to PHI and medical records. We have a set of strawman recommendations for us to discuss about this second bucket of issues, where the provider again discovers the error not prompted by the individual and what happens moving forward from that.

Then, the third bucket of issues are, what are the technical pieces of this that we might want to recommend. In particular, are there certification requirements, for example, that would help EHRs to be able to make corrections to information in the record or to pass on a message successfully about an error in the records so that subsequent providers can see it and can act on it? In essence, the technical piece of how a correction or an amendment or a notation gets propagated downstream is, it’s a similar set of technical issues regardless of whether you’re talking about a correction that an individual has requested or a correction that is discovered by a provider. In essence, this document repeats the technical issues in both with respect to both sets of issues, but I think they’re similar. Of course, we could disagree in discussing this and decide that in fact they're not similar at all, but at least in developing these strawman policies, we sort of consider the technical pieces to be quite similar.

So I'm going to propose that we focus our discussion today on the what I'm calling the second substantive bucket of issues, which the policies around correction for which we don't have any guidance in HIPAA. That is the principles for other changes to PHI and medical records, the errors that are discovered by a provider and what if any are their notification obligations with respect to data that they correct. Paul, did you want to add anything before we open this up a bit?

Paul Egerman – Software Entrepreneur
No. It's a good discussion.

Deven McGraw – Center for Democracy & Technology – Director
Okay so essentially what, again, with some help from team MITRE we've come up with some strawman recommendations here that begin with establishing a responsibility to identify potentially inaccurate and incomplete PHI and notifying the source of that information of any potential gap.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Could you walk us through how this looks from the point of view of a doctor and the small practice who's just received some information through the HIO?

Deven McGraw – Center for Democracy & Technology – Director
Through an HIO? So, okay, that's one way to do it. So the way it looks is that if I get information as a small practice provider and I think it's an error, but it's not my source information. I got it through the HIO but presumably the HIO isn't the source of the information either but knows the source of the information, that they would notify the source that there's an error in the data.

Paul Egerman – Software Entrepreneur
Either an HIO notifies the source or maybe the provider would directly notify the source of the HIO.

Deven McGraw – Center for Democracy & Technology – Director
It doesn't say that actually, so recognizing that HIOs or business associates so they're purchaser paying providers. One could presumably rely on an HIO if you use one to make the notification if that's part of the participation agreement. But inevitably the obligation is for you to notify the source of the error.

Paul Egerman – Software Entrepreneur
Right, especially if the HIOs a federated model. The HIO may not have any data at all.

Deven McGraw – Center for Democracy & Technology – Director
Well that's right. But even if it does, it doesn't create data.

Paul Egerman – Software Entrepreneur
Hopefully.

Dan Rode – AHIMA – VP Policy & Government Relations
Deven, I think in that scenario, the one thing to remember is that the party that became aware of it needs to potentially correct or amend the data has to be able to talk to the source party because it could in that conversation, whether it's electronic. Or you just pick up the phone, could be determined that a correction should not be made and so having an interim body in the middle, really just complicates the communication ... there.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So, there's enough doctors on the call that I can speak without fear of an error standing uncorrected here. I see this as an increase in workload for people who right now often don't report events that they should because of the time that it takes to report the events. So I'm wondering is this, I mean, there's no question about the value of it, I guess the question is I can see life threatening situations. It says there's

no information on a patient's allergy to seafood or penicillin, but there's a statement that there's no known allergy and that represents a certain amount of threat to the patient if it's not corrected. But then, there are others where, yes, it's wrong but the likelihood is that before it gets misused, it will get verified and so forth. I just feel like it's potentially something that's going to be honored more in ... than in reality if we're not careful here, if we're not balancing the benefit with the intrusion.

Deven McGraw – Center for Democracy & Technology – Director
That brings up a question that we tried to key up a little bit later in the discussion, but we don't have to wait till later to bring it up. That is whether we would want to, in terms of the obligation notify, either backwards to the source or downstream to providers that you know have received it. Whether there ought to be a thresh hold so that it's not every error potentially but ones that—and you raised the possibility, have implications for patient care or where a failure to notify could be detrimental to the patient.

Judy Faulkner – Epic Systems – Founder
Can I give another scenario because we're finding this to be a real life scenario here? We may have 25 different, patient having seen over a number of years, 25 different small individual providers. Each one with obligation to share the data. The providers really don't want to see each other's data. They're afraid of giving 15 minutes to see that patient, they have to read through 25 separate evaluation write-ups about the patient from each of 25 different doctors and somehow in their brain put that all together and figure it out. So we're seeing that what the physicians want to do is not see each other's information.

Deven McGraw – Center for Democracy & Technology – Director
Okay well Judy, I mean I'm not sure how to address that because it gets at the heart of whether information ought to be exchanged in the first place.

Judy Faulkner – Epic Systems – Founder
Yes. It does.

Deven McGraw – Center for Democracy & Technology – Director
And whether the way that it's being exchanged is being done in a way that is efficient for providers to look at.

Judy Faulkner – Epic Systems – Founder
Yes. And this is a real life situation we're running into.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I get that but that seems to me to be maybe getting at Wes's question about maybe a little bit to Wes's question about whether what are we asking of overtaxed providers in terms of notification.

Judy Faulkner – Epic Systems – Founder
Yes. And what they want us not to present it to them because they don't want to have not looked at it. They want it not to be there.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
This would be another reason not to want it presented is if I have an obligation to try to correct 25 doctors going back over 10 years. I think that the notion that this principle, which is only a principle until some regulations come out or something, is needs to somehow be described value or threat or something like that is true. I think that Judy raises the much larger issue, which goes to a similar issue, which is I think that most physicians that I've talked to would say there's some percentage of the cases, higher for ED physicians and even then probably less than 10% of their cases. Where they do want to see other information but that's specific they want to be able to ask with some kind of specificity. They don't want to just see a dump of every ear infection that the kid's ever had.

Judy Faulkner – Epic Systems – Founder
Right. They want to look for what's relevant to what they're doing.

Paul Egerman – Software Entrepreneur
That's critical to the whole notion of the ACOs and all of the shift away from fee for service. They're going to have to look at other data and coordinate or they're not going to be players.

Deven McGraw – Center for Democracy & Technology – Director
No that's absolutely true but I don't know that we were presuming data dumps, and if it looks that away from the recommendations that is not at all what we're trying.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think that's—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I wanted to go back to Wes' original question. Isn't what Wes described already HIPAA policy that the downstream provider who receives something in error is--?

Deven McGraw – Center for Democracy & Technology – Director
No.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So this would be an extension.

Deven McGraw – Center for Democracy & Technology – Director
Yes. The obligation to notify is with patient, with respect to patient request for communication, not errors that you spot that are unprompted by a patient.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Okay. I just now figured out the color-coding of this document.

Deven McGraw – Center for Democracy & Technology – Director
No. it's okay. This entire section begins on page four if you print it out and it's highlighted on the screen is the one that deals with this is all new stuff in bold. It's really referring to not an obligation, I don't think, to scan for errors, but when you see that, what is your obligation when you see something that is wrong? Maybe we might need to step through this very carefully. What's your obligation when you're not the source? What is your obligation when you are the source?

Paul Egerman – Software Entrepreneur
And if I'm hearing Wes' comment correctly, this is Paul, and also picking up a little bit on what Judy is saying. In terms of obligations of user source of the recipient when information is exchanged as it relates to potential errors, there ought to be some threshold that's subjective, that the party states that it's important to communicate that they don't necessarily have to communicate everything.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
One solution would be to say that there must be an easy way to send that feedback not an obligation to send it. For example, I was thinking of my own examples. The patient might be a, as I understand it, the patient is allergic to seafood then some contrast medium can be quite dangerous to the patient, but a physician may believe that no radiology practice in good standing would ever use the contrast medium without asking at least three times about the patient's allergies. So that's sort of the subjective need to invest time in making sure that information gets back and the need at the receiving end in evaluating all incoming information and deciding how to deal with it, seems to be quite subjective.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I had another thought on this as well, which I'm concerned about. How do you distinguish between an inaccurate or incomplete PHI and a case where you might have a good faith difference of opinion about a diagnosis or something of that sort? I mean that happens all the time where two professionals may have a disagreement as to the underlying ailment that a patient has or something related to the patient's

treatment. Frankly, the thought that where does one, start at one end in terms of what's an error versus what is a difference in opinion, I think could be quite problematic in the context of this.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I think those drawing those lines will be difficult. The MITRE folks tried to help us out a little bit with some definitional terms in the beginning of the document but even if you say that a correction is something that replaces erroneous information with accurate information, if you have a genuine dispute about a diagnosis, that definition doesn't help you very much.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
... lies in the correction systems.

Dan Rode – AHIMA – VP Policy & Government Relations
Deven, this is Dan Rode again.

Deven McGraw – Center for Democracy & Technology – Director
I don't know that we can or would want to replace clinical judgment about an entity or a provider's own record and what information is in it, right?

Paul Egerman – Software Entrepreneur
I think was Dan was trying to—

Dan Rode – AHIMA – VP Policy & Government Relations
I wanted to mention that in John's case, if we look at the models we're headed towards, if a primary physician were to send a patient to a specialist who essentially looks at it and says oh that's not right. Typically, the specialist would be sending some type of a letter back to the primary physician. I say letter because that's still a favorite ... but some type of report back to the primary care physician which would get added to the record, wouldn't change anything but it would be an addendum essentially saying on further reflection, this is what we think the diagnosis is ....

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
... if there was a consultation done or somebody's going to a specialist, I could understand that but I think there's an enormous number of context where, data in a record might be doubted by a physician as part of a more general review or in a context that isn't quite as clear cut as that. I just think there's a lot of cases where it could occur, physicians simply mentally checks it off as not necessarily even being, he or she being in agreement with they might note it in the record differently and the thought that then we might have to remember to go follow-up could be incredibly burdensome and difficult.

Dan Rode – AHIMA – VP Policy & Government Relations
And there's no disagreement there, and I think that's one of the reasons that we want to see more and encourage more patient involvement. If the patient feels it's necessary to go back to the individual physician, the previous physician down the line, then they have an obligation as well.

Paul Egerman – Software Entrepreneur
And to keep ..., make sure we're all on the same page, we talk about specialist and disagreements about diagnosis, we're talking about across entity boundaries, right? So, I just want to make sure we're talking about across entity boundaries and since it is across entity boundaries it's also, at least theoretically, possible that one entity has a different list of diagnosis on the patient and another entity has. They just disagree.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Actually, or it could be a different ICD 9 code.

Paul Egerman – Software Entrepreneur
Different ICD 9 code or possibly like a different description of the intensity or severity of the illness.

Dan Rode – AHIMA – VP Policy & Government Relations
Well that can happen to the entities too.

Paul Egerman – Software Entrepreneur
But that's not necessarily a correction.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Paul and Deven, can you hear me?

Deven McGraw – Center for Democracy & Technology – Director
I can now. Not very well though. It needs to be a little bit louder.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I'm really confused by this conversation because it sounds like we are having a conversation about getting to a single medical record that is the source of all truth, and I don't think that's the topic for this discussion. There will always be differences of opinion between clinicians. Those opinions will change overtime, diagnoses may change over time, that's the nature of health care. I'd love to see us just get back to the topic of a true error.

Paul Egerman – Software Entrepreneur
Yes. I think Carol, I think you're exactly right, but the reason I was trying to point out the entity boundaries. It's not like there is one description of truth as it were, and there are some true errors and the issue is that there's a lot of them, and what are the obligations of the party, number one. And number two is do we need to consider any technology or certification kinds of requirements as it relates to corrections. And—

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Well I think it would help this discussion if we could talk about and maybe this is something we could be provided, the classes of errors we're considering and really define them. So is one class of error, I send the lab results for the wrong patient to you? I mean, it would really be helpful to just classify what we mean by error and narrow it down to just the classes because I think we could spend a lot of time on trying to come up with different scenarios that I don't think are reconcilable.

M
Yes, I just. My concern though, Carol, is simply that this isn't black and white. There's a lot of grey areas and I'm concerned that there's room for a lot of difference in opinion and—

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Fine. But the grey areas is the nature of health care. Right? Because some people carry a diagnosis for six months to a year before somebody really figures out what's going on and that diagnosis changes. In some ways, that's just an artifact of human beings. So I just want to make sure that when we talk about errors, we're talking about specific classes of errors for which we believe a correction is necessary.

Paul Egerman – Software Entrepreneur
Right and that is what we're talking about. I had a previous discussion with Deven and Joy on this topic and I used it as an example ... example I remember was an encounter note, and the patient was being status post tonsillectomy. You read the note and in the note it says some description of the patient's tonsils. The tonsils appeared to be normal. So the question is where were they, were they in a jar? The patient had a tonsillectomy. So clearly the physician is a human being that was busy and made a mistake. It's just that simple. ... is also the example that one while this may be an embarrassing mistake, probably didn't have a lot of clinical significance, right? It's just you kind of would like to fix it because it's embarrassing but it's not a big deal.

Judy Faulkner – Epic Systems – Founder
So how do we tighten up the language to make it specific to those things that are critical and we don't overburden the doctors?

Deven McGraw – Center for Democracy & Technology – Director
Yes. I mean I think in two ways, Judy, and two of which have been thrown out. One is to define with a little bit more specificity what we mean when we say correct error. What's an error? Correct something that's not accurate versus what's a reasonable difference of opinion among providers about an accurate diagnosis, for example. Then, the other one that's been thrown out is that the thresh hold for any notification of a correction even of an error be one that would have an impact on patient care if it was not disclosed.

Judy Faulkner – Epic Systems – Founder
But how could we, could we tell the doctors what it is?

Paul Egerman – Software Entrepreneur
It would be up to their judgment.

Judy Faulkner – Epic Systems – Founder
Oh I think that that leads us to litigation.

M
I mean I think you're there already. You have a duty as a physician to look out for the best interest of your patient. If you discover a major error being propagated like left kidney instead of right kidney—

Judy Faulkner – Epic Systems – Founder
And I maybe we put in major error because my worry is that after the fact, who's going to say something about an allergy that one thought was there and another one actually didn't think was there, which is right is it a major error. You could say that that's a fact that's disputable but maybe it is an error maybe it's not a fact. I mean maybe, I'm not saying that.

Deven McGraw – Center for Democracy & Technology – Director
I don't know. I appreciate where you're trying to go Judy, but I'm not sure the addition of the word major helps. They're still going to have to make a judgment call about what's major and what's not.

Judy Faulkner – Epic Systems – Founder
So there I am, I'm a physician, I have many, many different things in front of me and I'm skimming through them quickly from different places trying to find what's relevant to my care and I see different things and different ones. It says different allergies, different, there's lots of different forms that I'm looking through to find out what's real and what I have to do to this patient and I see discrepancies and they still appear to be errors. What's my obligation?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I am thinking that we need a formulation that focuses less on the obligation of the physician to act and more of the obligation of the service providers to make it easy to act. In other words, it's not clear that under the privacy and security policy, we have the right to point of view to be discussing when a physician should decide to report something back and when they shouldn't. But if we grant that there are cases that physicians may conclude they need to report back, then we can create policies or regulations that make it much less of an investment of their time to do so and perhaps increase the fidelity of that information getting back. So that might save us a lot of discussion on essentially imponderable issue and allow us to focus on where we actually know something.

Deven McGraw – Center for Democracy & Technology – Director
That's a really interesting idea, Wes. That rather than asking providers—but would you confine it just to reporting back versus you discover an error that you've made and what is your obligation to—?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
No, I wouldn't. I just, that was where the conversation's been going, but I just think that there's a difference between the mechanism and the obligation. When a patient initiates or request, it's clear that

HIPAA provides guidance on what the obligations are. I think if we focus on just this is very similar I think to studies that have been done on adverse events that if you can make it far easier to report an adverse event, adverse event reporting goes up. I think we similarly could say if we could make it far easier to deal with an error, either one discovered in one's own work or one discovered in providers' work but leave the actual decision to act to the judgment of the physician where it will be anyways no matter what we write. Then we can probably have a more productive discussion.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It seems logical to me to nail down the forward propagation of a correction before we try to wrestle with the back propagation of a detected error that was detected downstream. Are we comfortable that we have a model in place for forward propagation of corrections or is that also on the table for discussion?

Deven McGraw – Center for Democracy & Technology – Director
Well I mean that's why I asked Wes the question, David, because the only cross set of requirements that are in place for forward propagation have to do with when a patient requests a correction and then HIPAA already has that handled. I thought I heard Wes saying let's not touch judgment calls about whether errors need to be corrected either backwards or forwards and instead just focus on the technical capabilities to be able to provide that notification should you decide to do so but I also may not have—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well I, yes, in essence I'm saying that the decision on whether an error must be corrected regardless of backwards or forwards or sideways, is a very hard issue to try to wrestle to earth. The decision on whether standards should allow for the provenance of information that is sufficiently specific to allow that reporting whether HIEs that are in fact HIOs I guess we're calling them now, that in fact provide intermediate access to information that's literally not known to the provider who got the information. The fact that they maybe should have the standards and capability to record those and be able to forward propagate errors. I think or reports, I think that's more—If we don't do the second part that I'm describing, the first discussion is irrelevant. If we do, we know we've at least changed the decision process of the provider in favor of reporting what's important in their opinion or correcting what's important in their opinion and that's a big step forward.

Paul Egerman – Software Entrepreneur
I'm listening to what you're saying Wes and it makes a lot of sense to me, especially in the environment where we're trying to encourage information exchange, and if we start to put forward some series of difficult obligations, that's the opposite of encouraging. If I'm hearing you right, it's almost like we need a new color button instead of like a blue button some other color button. Some in effect button that the physician pushes if he sees something that doesn't look right that says I thought the patient was a female but this says male, and it handles it for the person rapidly.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I keep coming back to the simplest use case is to ensure that locally made change, whether it's a correction or addendum or whatever is propagated downstream according to standards that allow for that to happen. I mean, if interfaces aren't being created that can support propagation of corrections forward, everything else, we shouldn't even bother with.

Paul Egerman – Software Entrepreneur
Yes. But there's still an issue even there, right? Because what are the changes you have to propagate going forward?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
And that's what we think that even the simplest case to take on is for example just make up strawman here is you could certify that EHR is able to propagate according to a defined standard and addendum or correction to a CCD or a document or a lab result. I think most interfaces can do that already, but until that's nailed down, it seems like it's really going to be hard to make it go backwards where there is not a standard interface flow. We suddenly, we shouldn't take that on but are we comfortable that we've got the distribution forward case covered?

Carl Dvorak – Epic Systems – EVP

I would just be careful to recognize the enormity of what we're really talking about. It sounds easy on the surface but as you really get into chart corrections and we've done a lot of work in this area, it is enormously complicated for a couple reasons. One is that any individual data item of a trivial contemplate changing it, it often has ripple effects across other data that was derived or used subsequent to the original entry. Then secondly many kinds of changes would actually necessitate a provider reviewing that patient's record and reviewing the case in general to look for what other decisions might have inaccurately been made or what other decisions might have been made on that inaccurate data.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Carl, I appreciate how hard those interfaces are to write, but I think the fact that it's hard doesn't mean that you don't propagate what you can propagate. You may ... that reverse ... but you can propagate a correction if you know it.

Carl Dvorak – Epic Systems – EVP

I think I agree with you David, on one level. The technical propagation is not that complicated but you have to account for a lot more than just the technical propagation. We may want to start simple with propagating and addending entry to let someone know that the chart has been, a request has been made to modify the chart and to what level and what the origin of that request is and try to keep it, I don't know, appropriately reasonable to start with. I think you'll quickly get into an abyss that we won't get back out of for several years, and yet there are probably some very straight forward things we can do to achieve the objective of letting people know something relative and important has changed or needs to change in their understanding of that patient.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And I'm talking mostly about what you would call technical propagation. I don't think we can certify legislate or otherwise influence necessarily the actual behavior of the people downstream who see it, but we can at least assure that—

Deven McGraw – Center for Democracy & Technology – Director

The information gets there.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

The information gets there in a standardized way. It may not cover every single, possible use case, and I think most interfaces do that already. I don't think I'm asking for something that's out of scope of what most of them do. But that's a starting point. And then the second thought, I'm seguing a little bit here is the provenance work that's being done as a downstream aspect of the ... report by the other work group is an interesting place to think about as a nexus for the back propagation as I think Wes was hinting. As you could put information in there for example including the address if you would, the direct address maybe someday of the provider that created the document so that you could in fact have a channel back that follows the document along. But I'd start with the moving the data forward and then worry about how to get it to go backwards.

Judy Faulkner – Epic Systems – Founder

I like the idea of we have to reconsider what the patient wants us to change and we have to move forward. I think that we have to realize the doctors are professionals. They do this and leave it up to them to decide what is relevant going backwards and what isn't and that we shouldn't be addressing that at all.

M

I agree.

Deven McGraw – Center for Democracy & Technology – Director

Yes. This all seems to be coalescing around some common themes here except in one area where I'm still a little confused. Are we or are we not deciding that we would put a substantive requirement, forward propagate a correction that you discover in your data and think is relevant to patient care for downstream providers? Because initially it sounded like we wanted to leave all of the judgment calls about whether information goes either backward or forward up to the provider but at least put in their hands the technical tools for moving information about a potential error forward.

Judy Faulkner – Epic Systems – Founder
Deven, could you please define forward propagate?

Deven McGraw – Center for Democracy & Technology – Director
Okay sure. I'm the nontechnical person here and so I may need some technical help on it, but when I think about backwards propagation, I think I'm the recipient. I'm the provider who's received data from somebody else and I think there's an error in it. It tells the original source provider that there's an error would be in my view propagating backwards because it's not my data. I have to tell the source. I might correct it, and I might do something with my own record to reflect what I think is accurate data, but I've decided that I want the source to know that it's an error because for whatever reason I think it's important. The patient care I think it's actually—I'm pretty confident that I'm right and that was an inadvertent error on their part. So that's backwards. Then for forwards, it's oh I just discovered and maybe it's Paul's example about the tonsils or maybe it's I've discovered that I put in the wrong gender for this patient. And I shared the record yesterday with the specialist who is also in my accountable care organization, so I'm going to let her know that in fact the record I sent her yesterday had an error in it, which is I put the patient's gender in there wrong. And maybe forward's a bad example because it's not—

Paul Egerman – Software Entrepreneur
Well, let me give like a different, to give a different example that might be—

Deven McGraw – Center for Democracy & Technology – Director
Thank you Paul.

Paul Egerman – Software Entrepreneur
Might be realistic. But let's look at a situation where a patient's discharged from acute care institution, transferred to an extended care facility and in that process a discharge summary is created on the patient. I think it states to, we're going to electronically transmit those discharge summaries. So the discharge summary goes from the acute care hospital to the extended care facility. So the source is the acute care hospital. The destination is the extended care facility, and the forward propagation would be after you discharged the patient and after you submit the discharge report, you discover that something was missing. Maybe you have one of these classic things, the discharge summary was created by a resident. It was created in a hurry because they were stressed about discharging the patient. It was signed by the first attending anybody could find. They got the patient out the door, and then the next day they realized they made a mistake. So correcting that mistake would be forward propagation because we go from source to destination.

Backward propagation would be the patient gets over to the extended care facility. They look at the discharge summary. Say it doesn't make sense. This is not the right set of drugs. They contact the hospital. They do something to try to get the thing corrected, which might be important to do because the patient may eventually be readmitted.

Judy Faulkner – Epic Systems – Founder
Well Paul and Deven, what I've seen in common with both of your definitions is that backwards propagation means correct somebody else's and forward propagation means correct my own.

Paul Egerman – Software Entrepreneur
Now backward propagation would mean notifying the source that there's a potential error. It's still their responsibility to fix it.

Judy Faulkner – Epic Systems – Founder

So going forward, I guess what I don't get about what you're calling forward propagation is what you're saying is I found that I did something wrong, I have a responsibility to correct what I did, which I would think is there already. If you said it's female and it's male or vice versa then in fact you have an obligation, if you discover that, to fix it and not later on to be saying oh well yeah, I knew it was wrong but I didn't fix it.

Paul Egerman – Software Entrepreneur
Close enough.

Judy Faulkner – Epic Systems – Founder
That doesn't make any sense then.

Deven McGraw – Center for Democracy & Technology – Director
Okay well—

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Can I just jump in here for one second and say that I agree with that questioning? I also want to say that the most important error to correct. if there is one is at the source. I don't know how we're using the term propagation but if you want to prevent that error from propagating again and again and again, it is important to notify the source. I would just put some emphasis on that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think I introduced the word propagation, and I certainly agree with Judy that all systems allow you to correct the data within the system. I'm saying should we, and I'm asking as a question should we certify for capabilities to pass that correction forward across standard interfaces? Maybe there's a subset where we would say we should live interfaces, continual interfaces. Maybe there's a subset where you can't because it's one-time transfer and you don't have a standard interface but it seems to me that's a fundamental question that's technically within scope most interfaces, in fact, do propagate corrections across the interface. And they propagate enough identifiers to make it easy to reconcile a correction on the downstream system, but I don't think there's any notion that that's a requirement yet.

Leslie Francis – NCVHS – Co-Chair
Can I just throw one more thing in? Which is from a privacy perspective, we're of course concerned about correcting errors for patient care, which would suggest that upstream forward looking is what matters more, but we're also concerned about errors that might have deleterious other source of effects on patients. For example, an error that indicates the diagnosis of serious illness, which is false, but that might turn out to be very problematic if a patient applies for insurance. So I just want to make sure it's out on the table that correction, whether if comes from the physician or from the patient is not just about medical management in the future.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think you can go the other direction as well and say that there is information that can be life critical that isn't an error itself but it's just completion of a slow to resolve result. A classic being a tuberculosis culture, which sometimes take six weeks, and if the positive culture is never propagated forward, you've got a patient out there infecting people. It happens all the time.

Paul Egerman – Software Entrepreneur
David, that's not a correction. That's just an update. That's just the way health care works. Some things take longer than others and the data set is constantly changing based upon new information that you have.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No I agree. I'm saying it's an update but it falls in the same technical capacity. If you have the capacity to propagate an update like that across say to an HIE, then you can also propagate corrections.

Judy Faulkner – Epic Systems – Founder

Aren't we getting into a complex thing here, which can take us a year to do, perhaps, as we go into all ramifications of this and should we just go back to the patients having a correction to the records?

Deven McGraw – Center for Democracy & Technology – Director
I don't know Judy. We may in fact be in that spot, but we've only spent about an hour on one call. So I'm actually not ready to throw in the towel quite yet. I think there were—Let me ask Dan. Dan Rode, are you still on the phone?

Dan Rode – AHIMA – VP Policy & Government Relations
Yes. I'm still on.

Deven McGraw – Center for Democracy & Technology – Director
So in terms of whether or not there are already a set of existing obligations on providers, if they discover an error in data that they created and sent on, do they already have a duty under some law—? We know it's not under HIPAA, but do they already have a duty to inform others that they know they've shared it with of the corrections?

Dan Rode – AHIMA – VP Policy & Government Relations
In the context of this conversation, there may be some state law that I'm not aware of but I'd say it's more of an ethical issue than a legal issue.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

Paul Egerman – Software Entrepreneur
Right.

Deven McGraw – Center for Democracy & Technology – Director
So I think the other piece of information that might help us come to resolution on this is whether it's how if at all some of the health information exchanges have handled this issue with respect to the participants. Because what I'm hearing is—and I'm not doubting you, Judy, that it's problematic. We may in fact not be able to come to some consensus on resolution of the policy issues, although there appears to be some consensus building for at least a first level technical fix that allows for some information to be sent forward that indicates a correction to the record or previous information that was sent. But in terms of setting a policy recommendation forward such as one that we might suggest be adopted as part of NwHIN, what potentially would that look like in terms of when errors are spotted in creating a genuine obligation for people to notify versus just bounding it in ethics?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Deven, are we speaking about errors discovered by both the provider and the patients essentially or just the provider?

Deven McGraw – Center for Democracy & Technology – Director
I'm speaking of just the provider only because we actually do have a set of requirements in HIPAA already for when the patient sees what he or she thinks is an error and asks the provider to correct it.

M
So Deven, playing on that logic there, so what it let's say since we have to honor the patient's wish, what would be the system implementation of that and how would that be different from propagating provider initiated corrections?

Deven McGraw – Center for Democracy & Technology – Director
Yeah I actually don't think it is, from a technical standpoint. So I sort of feel like, Wes had to drop off the call, but I feel like we're getting back to Wes' point a little bit, which is that we have a set of obligations about patient requested corrections. We want to make sure there's a technical capability to facilitate that. When we put that technical capability in place, we've opened the technical pathway for provider-initiated

corrections to flow as well but without necessarily putting a requirement for people to inform others of an error that they, providers themselves discover.

M
A difference in legal burdens?

Deven McGraw – Center for Democracy & Technology – Director
Right. Distinction. Because it sounds like people are on board with a technical way to implement what is already law on the individual side that will help facilitate notifications even of errors that are discovered by a provider but do we want to put an obligation on providers to alert of errors that they discover?

Judy Faulkner – Epic Systems – Founder
Well, I think that providers already have that obligation to alert others of anything that they think will harm the patient's health and that's called the Hippocratic oath.

Deven McGraw – Center for Democracy & Technology – Director
Yes. We don't have a way to hold people accountable to that though. But it's a good point.

Paul Egerman – Software Entrepreneur
Yes, but that point that Judy's making is consistent with what Wes is saying, which is all we need to do is to make sure the right technical capabilities are in place. We don't really need to try to specify new obligations on the health care professionals.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, and it's consistent with me as well. I think provider's judgment will determine how much effort should be expended based on the urgency of the correction, but we can put in place technical solutions that make it possible to do it and in some cases it should probably just be automatic, what I was calling forward propagation should just be no thought because it happens.

Paul Egerman – Software Entrepreneur
Well there's also some issues that we haven't discussed. We've only looked at these issues so far in terms of information exchange, but as we think about corrections, I think we also have to ask whether or not there's any EHR certification criteria that's needed for the EHRs themselves. So new obligations in the part on the part of the clinicians. Another thing that we've heard is we need to focus on making it technically possible to communicate information about potential corrections.

Another thing that I think we heard from David is a certification capabilities for make sure that the systems have the capability to propagate a change to if they sent out something, a CCD or discharge summary. That there's a capability to send forward a corrected one without specifying why they have to do that or when they have to do it. Just make sure that they have the capability to do it. And then, I'm raising the issue of at least on progress notes, is within the EHR, is there a, do we need to do certification criteria to make sure that somehow notes are finalized that say provenance is maintained when you transmit information that perhaps the audit trails are kept prior information? Is that a good summary or is that not a good summary?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that's a good summary. It's funny that we took on the hardest one first and worked our way back to the one that's probably easiest.

Paul Egerman – Software Entrepreneur
That's actually an implementation technique that sometimes is used.

Judy Faulkner – Epic Systems – Founder
That's reasonable Paul.

Deven McGraw – Center for Democracy & Technology – Director

That was a nice summary and articulation Paul, and what I would suggest that we do is work forward from that list in terms of any additional wordsmithing or any additional details that we might want to make for those four categories, also at our next meeting which is June 3. It also lets us sit a little bit with this discussion and make sure we're okay with what we're putting forward. Did I just completely not make sense or are people okay with that?

<u>David McCallie – Cerner Corporation – Vice President of Medical Informatics</u>
No it makes sense. It sounds reasonable. This is David.

<u>Deven McGraw – Center for Democracy & Technology – Director</u>
Thank you. I don't know whether people are dead tired or I didn't make any sense.

<u>Paul Egerman – Software Entrepreneur</u>
No. we were trying to decide whether a response was forward or backward. That was the only problem. And so, we were unsure.

<u>Deven McGraw – Center for Democracy & Technology – Director</u>
Okay that's completely fair. That's what I propose we do for June 3rd is we'll work offline to un-pause articulation of the four points that we want to make and we have to spend our last meeting before the June Policy Committee meeting adding any bells and whistles to that that we want to so.

<u>Paul Egerman – Software Entrepreneur</u>
So that's great, and this has been a great meeting.

<u>Deven McGraw – Center for Democracy & Technology – Director</u>
It really has.

<u>Paul Egerman – Software Entrepreneur</u>
We had an interesting discussion about corrections. We talked about our topics going forward and dealt with the intriguing issue relating to certificate authorities. So Deven, are we ready to look at—?

<u>Deven McGraw – Center for Democracy & Technology – Director</u>
Public comment?

<u>Paul Egerman – Software Entrepreneur</u>
Public comments.

<u>Deven McGraw – Center for Democracy & Technology – Director</u>
I believe we are. Judy?

<u>Judy Sparrow – Office of the National Coordinator – Executive Director</u>
Okay, here we go. Operator, can you check and see if anybody wishes to make a comment.

<u>Operator</u>
We do not have any comments at this time.

<u>Judy Sparrow – Office of the National Coordinator – Executive Director</u>
Okay. Thank you all and thank you Dan.

<u>Paul Egerman – Software Entrepreneur</u>
And thank you Judy Sparrow and Deborah Lasky, if you're still on the call, thank you very much again for all of your help, and thanks to all the tiger team members. See you on June 3rd.